What is claimed is:

1. An apparatus for encryption/decryption (200), comprising:

a keyschedule unit (201) for a Cipher Key, said keyschedule unit (201) providing a predetermined number of expanded key values, said keyschedule unit (201) having a memory (202);

a conversion module (208) in communication with the keyschedule unit (201), said conversion module converts a block of plain text/ciphered text into a predetermined number of byte units in a first plurality of columns;

a block round unit (212) for encrypting/decrypting the predetermined number of byte units into ciphered text/plain text; and

a key expansion module (215) for performing key expansion on both normal (encryption) and inverse (decryption) functions to obtain expanded key values;

wherein a number of memory spaces in the memory (202) required for storage of the expanded key values is no greater than half the number of expanded key values.

2. The apparatus according to claim 1, wherein the predetermined number of expanded key values equals 14 and the number of memory spaces is equal to 7 without an increase in access time relative to an equal number of expanded key values and number of memory spaces.

3. The apparatus according to claim 1, wherein the predetermined number of expanded key values equals 12 and the number of memory spaces is equal to 6.

4. The apparatus according to claim 1, wherein the predetermined number of expanded key values equals 10 and the number of memory spaces is equal to 5.

5. The apparatus according to claim 2, wherein a key length of the Cipher Key is 256 bits.

6. The apparatus according to claim 3, wherein a key length of the Cipher Key is 192 bits.

7. The apparatus according to claim 4, wherein a key length of the Cipher Key is 128 bits.

8. The apparatus according to claim 1, wherein a key length of the Cipher Key is greater than 256 bits.

9. The apparatus according to claim 1, wherein a rate at which the key values are expanded is synchronized with Round Key processing by the block round unit (235).

10. The apparatus according to claim 1, wherein the key expansion module includes means for expanding 14 keys such that keys 1 to 7 are sequentially expanded during encryption, with each expanded key value being used for processing a Round Key algorithm in parallel before another key is sequentially expanded.

11. The apparatus according to claim 1, wherein the key expansion module includes means for expanding 14 keys such that during decryption keys 14 to 8 are expanded in the memory spaces in descending location order, followed by expanding keys 1 to 7 in ascending location order, followed by keys 14 to 8 being re-expanded in descending location order.

12. The apparatus according to claim 11, wherein the memory (202) comprises no more than 7 memory spaces for storing the key values, and once key 8 is read from a location 1, key 7 is expanded and placed in location, wherein keys 7 to 1 are read in ascending location order and a Round Key Algorithm is performed in parallel with each key expansion.

13. A method for reducing memory requirements during a key expansion function, said method comprising the steps of:

(a) providing a keyschedule unit (201) for a Cipher Key, said keyschedule unit (201) providing a predetermined number of expanded key values, and said keyschedule unit (201) having a memory (202);

(b) providing a conversion module (208) in communication with the keyschedule unit (201), said conversion module converts a block of plain text/ciphered text into a predetermined number of byte units in a first plurality of columns;

(c) providing a block round unit (212) for processing Round Keys for encrypting/decrypting the predetermined number of byte units into ciphered text/plain text; and

(d) providing a key expansion module (215) for performing key expansion on both normal (encryption) and inverse (decryption) functions to obtain expanded key values,

wherein a rate at which the key values are expanded in step (d) is synchronized with Round Key processing by the block round unit (235) in step (c) so that each of the respective key values is expanded in parallel with a respective Round Key being processed, and

wherein a number of memory spaces in the memory (202) required for storage of the expanded key values is no greater than half the number of expanded key values.

14. The method according to claim 13, wherein the number of memory spaces in said memory (202) is equal to 7, and the predetermined number of expanded key values equals 14, without an increase in access time relative to an equal number of expanded key values and number of memory spaces.

15. The method according to claim 13, wherein the key expansion module provided in step (d) expands 14 keys such that keys 1 to 7 are sequentially expanded during encryption, with each expanded key value being used for processing a Round Key algorithm in parallel before another key is sequentially expanded.

16. The method according to claim 13, wherein the key expansion module provided in step (d) expands 14 keys such that during decryption keys 14 to 8 are expanded in the memory spaces in a descending location order, followed by expanding keys 1 to 7 in ascending location order, followed by keys 14 to 8 being re-expanded in descending location order.

17. The method according to claim 13, wherein the memory (202) provided in step (a) comprises no more than 7 memory spaces for storing the key values, and once key 8 is read from a location 1, key 7 is expanded and placed in location, wherein keys 7 to 1 are read in ascending location order and a Round Key Algorithm is performed in parallel with each key expansion.

18. A computer program product for reducing memory requirements during a key expansion function, said computer program product comprising a computer-readable medium of executable instructions comprising:

(a) executable instructions for performing a key expansion during one of encryption/decryption;

(b) executable instructions for processing Round Keys by a block round unit in parallel with the key expansion by a key schedule unit in step (a) so that for each expanded key a respective Round Key is processed in synchronization; and

(c) executable instructions for storage of the expanded key values such that a required number of memory spaces in the memory for are no greater than half the number of expanded key values.

19. The computer program product according to claim 18, wherein the executable instructions in step (a) for key expansion expands 14 keys such that keys 1 to 7 are sequentially expanded during encryption, with each expanded key value being used for processing a Round Key algorithm in parallel before another key is sequentially expanded.

20. The computer program product according to claim 18, wherein the executable instructions for key expansion provided in step (a) provides instructions for expanding 14 keys such that during decryption keys 14 to 8 are expanded in the memory spaces in a descending location order, followed by expanding keys 1 to 7 in ascending location order, followed by keys 14 to 8 being re-expanded in descending location order.

21. The computer program product according to claim 18, wherein the executable instructions in steps (a) and (b) includes that the memory spaces comprise no more than 7 memory spaces for storing the key values, and once key 8 is read from a location 1, key 7 is expanded and placed in location, wherein keys 7 to 1 are read in ascending location order and a Round Key Algorithm is performed in parallel with each key expansion.